

AO 91 (Rev. 11/11) Criminal Complaint

AUSA Michelle Petersen (312) 886-7655

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

**FILED**

JUL 05 2017

UNITED STATES OF AMERICA

v.

CAMERON YORK, also known as  
"Curtis Jones"

CASE NUMBER:  
UNDER SEAL

THOMAS G. BRUTON  
CLERK, U.S. DISTRICT COURT

**17CR 450**

CRIMINAL COMPLAINT

**MAGISTRATE JUDGE**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning not later than in or around July 2016, and continuing until in or around May 2017, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant violated:

*Code Section*

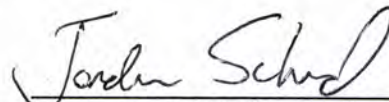
Title 18, United States Code, Section  
1343

*Offense Description*

Knowingly participated in a scheme to defraud and to obtain money and property by means of material false and fraudulent pretenses, representations and promises, and caused an interstate wire communication for purpose of executing the scheme

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

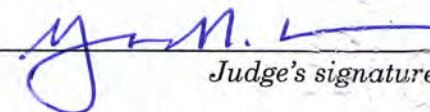


JORDAN SCHEID

Special Agent, Internal Revenue Service-Criminal  
Investigation (IRS-CI)

Sworn to before me and signed in my presence.

Date: July 3, 2017



Judge's signature

City and state: Chicago, Illinois

YOUNG B. KIM, U.S. Magistrate Judge

Printed name and Title

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS

SS

**AFFIDAVIT**

I, JORDAN SCHEID, being duly sworn, state as follows:

1. I am a Special Agent with the Internal Revenue Service - Criminal Investigation. I have been so employed since approximately 2011.

2. I am currently assigned to a High Intensity Drug Trafficking Area ("HIDTA") Task Force. Additionally, as part of my duties as an IRS-CI Special Agent, I investigate criminal violations related to financial crimes, including wire fraud, money laundering, and identity theft. I have participated in the execution of multiple federal search warrants.

3. This affidavit is submitted in support of (a) a criminal complaint alleging that Cameron YORK has violated Title 18, United States Code, Section 1343, and (b) a search warrant to search YORK's residence located at [REDACTED] [REDACTED]<sup>1</sup> (the "**Subject Premises**"), as further described in Attachment A. As further described herein, there is probable cause that (a) YORK has violated Title 18, United States Code, Section 1343, and (b) at the Subject Premises there exists evidence, instrumentalities, contraband, and fruits of violations of Title 18, United States Code, Section 1343.

---

<sup>1</sup> A copy of this affidavit that will be attached to the criminal complaint will redact the address of the **Subject Premises**.



4. The information contained in this affidavit is based upon my personal knowledge, as well as information provided to me by other law enforcement officers. It is also based upon my review of subpoenaed records, records obtained without the use of a subpoena, and on information provided to me by non-law enforcement personnel.

5. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging YORK with wire fraud, as well as probable cause to search his residence, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendant committed the offense alleged in the complaint and to establish probable cause to search the residence.

#### **SUMMARY OF THE INVESTIGATION**

6. The Federal Bureau of Investigation, the Internal Revenue Service - Criminal Investigation, and the Chicago Police Department are conducting an investigation of Cameron YORK and others, who have been fraudulently using personal identification information of third-parties and credit cards issued in the names of third-parties to procure hotel rooms, gift cards, and retail goods in the Chicago area. As part of his scheme, YORK uses gift cards and credit cards which he and others re-encode by saving stolen credit card information onto the card's magnetic strip.

7. As discussed below, YORK used the personal identification information of Victim A.F. to obtain an automobile loan for a Jaguar sedan ("Subject Vehicle"), and to open an account with a utility provider at the **Subject Residence**.

8. As further discussed below, YORK also uses fraudulent names and fictitious state identification cards to further his scheme, including the alias name of "Curtis Jones."

#### **I. FACTS SUPPORTING PROBABLE CAUSE**

##### **A. Cameron YORK's Possession of a Fraudulent Credit Card and a Fictitious Identification in the name of "Curtis Jones" During an Arrest by the Chicago Police Department**

9. According to information obtained from the Chicago Police Department ("CPD"), CPD officers, and CPD reports, on the evening of February 10, 2017,<sup>2</sup> CPD officers were on routine patrol in the area of the 4800 block of W. West End, Chicago, Illinois, where they observed a vehicle parked in front of a fire hydrant. When officers approached the vehicle, they observed the driver's side window to be rolled down and observed an individual smoking a brown rolled piece of paper that gave a strong odor of what the officers believed to be burning cannabis.

10. According to information from the CPD reports, there was only one occupant in the car. The police officers asked this individual to exit the vehicle and asked this individual for his information. At first, the individual claimed his name was "Cameron Jones," then claimed his name was "Cameron York," then finally claimed his name was "Curtis Jones." The man then produced a State of Illinois

---

<sup>2</sup> All dates and times in this affidavit are approximate.



identification card in the name of "Curtis Jones." As discussed below, the individual was later identified as Cameron YORK. The vehicle driven by YORK was registered to a female with the last name of YORK.

11. According to information from CPD reports, after YORK got out of his vehicle as the officers requested, YORK admitted that his real name is Cameron YORK and made a statement to the effect of that he uses the fake ID to get into clubs and uses fake credit cards to impress females at the clubs.

12. According to information from the Chicago Police Department, Officers placed YORK into custody for possessing a fraudulent identification card. YORK was also read his Miranda rights. CPD officers searched YORK's person and found a black iPhone and a Visa netSpend debit card with the name "Curtis Jones" and account number 432270xxxxxx3593<sup>3</sup> embossed on the card.

13. According to information from CPD officers and CPD reports, after YORK's arrest, the officer seized from YORK's person and YORK's vehicle, among other things,<sup>4</sup> an iPhone, a ZTE smartphone, the State of Illinois identification card in the name of "Curtis Jones"; and the Visa netSpend debit card in the name "Curtis Jones."

14. Additionally, on YORK's person, officers found a Nordstrom receipt from the Nordstrom located on 33 East Grand Avenue, Chicago, dated January 21, 2017.

---

<sup>3</sup> In this affidavit, portions of credit card account numbers and identification card numbers have been redacted.

<sup>4</sup> Additional items found on YORK's person or in YORK's vehicle included: a Western Union receipt, gift cards, International Money Orders, and bags containing a substance suspected to be cannabis.

The receipt shows a purchase of three items totaling \$644.96, including a \$160.00 t-shirt. According to the receipt, the items were purchased using a Visa card with a credit card account number identified only by the last four digits: xx7430. According to records obtained from Transunion, as of January 17, 2017, YORK had no credit cards in his own name, including no accounts with an account number ending in xx7430.

15. According to information from CPD officers and CPD reports, approximately two hours after arrest, a CPD officer interviewed YORK at a police station. The officer asked YORK about the fraudulent credit card and identification card that YORK had in his possession. YORK stated that he bought the credit card and the identification from an individual that lives in the neighborhood, Individual B, whom YORK identified by nickname. YORK related that he has Individual B's telephone number in his cell phone and usually communicates with Individual B via text message or through an application in his phone, though YORK could not recall the name of the text message application. YORK said that he paid \$100 for the identification card and the credit card. YORK said that he got the credit card and the identification card about two weeks ago and tried using the credit card at multiple gas stations, but the transactions were declined.

**1. "Curtis Jones" Illinois Identification Card**

16. According to CPD officers, the State of Illinois identification card presented by YORK was in the name of "Curtis Jones," listing an address in Glendale



Heights, Illinois and a date of birth of March 20, 1990. The identification number for this card ends in xx682J.

17. According to a search of information from a database of Illinois Secretary of State records, there is no valid State of Illinois identification card with a number ending in xx682J. Additionally, based on a search of that same database, there is no valid State of Illinois identification card issued in the name of "Curtis Jones" that lists an address in Glendale Heights, Illinois.

18. I compared the picture on the State of Illinois identification card in the name of "Curtis Jones" with photographs of Cameron YORK obtained from the Illinois Secretary of State identification card records and from Chicago Police Department arrest photographs. Based on this comparison, the photograph of the individual on the "Curtis Jones" identification card appears to be Cameron YORK.

## **2. Visa netSpend Debit Card**

19. Based on my training and experience, credit cards contain a magnetic strip, an electronic chip, or both a strip and a chip. The credit card account number is stored on the magnetic strip, electronic chip, or the strip and the chip.

20. Based on my training and experience, a credit card embossing machine can be used to emboss names and numbers on cards, making those cards appear as if they had been issued by the credit card company. Similarly, based on my training and experience, a credit card encoder can be used to encode the magnetic strip on the back of a credit card with a credit card number associated with a credit card account.

A credit card encoder can be used to change the account number electronically stored on the card's magnetic strip.

21. A CPD detective swiped the Visa netSpend debit card with the name "Curtis Jones" and account number 432270xxxxxx3593 embossed on the card through a magnetic card reader to determine the credit card account number encoded on the card. The credit card account number encoded on this card is 406095xxxxxx3593, which is different than the number embossed on the card.

22. Based on my training and experience, if the credit card were to be "swiped" using a magnetic card reader at a retail store or service provider, the credit card account number encoded on the reader, not the credit card account number printed on the card, would be the credit card account that would be charged by the business.

23. According to a law enforcement database, the account number stored on the magnetic strip is an account number issued by Navy Federal Credit Union.

24. On February 15, 2017, I spoke with a customer service representative with the Navy Federal Credit Union. The representative confirmed that a Visa credit card with an account number of 406095xxxxxx3593 was issued by Navy Federal Credit. Furthermore, the representative confirmed that Visa credit card with an account number of 406095xxxxxx3593 was not issued in the names of Cameron YORK or "Curtis Jones."



**B. Cameron YORK's Fraudulent Use of Credit Cards**

**1. Suspected Fraudulent Use of a Credit Card at Hotel A**

25. According to records provided by Hotel A, located in Chicago, Illinois, a reservation in the name of "Curtis Jones," listing an address in Glendale Heights, Illinois, was made for one room booked for two nights beginning on November 18, 2016.

26. As noted above, YORK was arrested by the Chicago Police Department on February 10, 2017 and was in possession of a State of Illinois identification card bearing the name "Curtis Jones" and the same address in Glendale Heights, Illinois as was used to book the hotel room at Hotel A.

27. According to Hotel A, the reservation was paid for using a Visa credit card with an account number ending in xx2607.

28. On February 16, 2017, I spoke with a representative from Citibank that confirmed that the Visa credit card with an account number ending in xx2607 was issued by Citibank. Furthermore, the Citibank representative confirmed that Visa credit card with an account number ending in xx2607 was not issued in the name of YORK or "Curtis Jones."

29. According to records provided by Hotel A, a second reservation in the name of "Curtis Jones" was made for two rooms booked for one night each beginning on December 2, 2016. The records provided by Hotel A for this reservation do not provide a full address for "Curtis Jones," but only a city and state of Glendale Heights, Illinois.

30. According to Hotel A, this reservation was paid for using a Visa credit card with an account number ending in xx5057.

31. On February 16, 2017, I spoke with a fraud investigator from Synchrony Bank that confirmed that the Visa credit card with an account number ending in xx5057 was issued by Synchrony Bank. Furthermore, the Synchrony Bank fraud investigator confirmed that Visa credit card with an account number ending in xx5057 was not issued in the name of YORK or "Curtis Jones."

**2. YORK's Use of a Suspected Fraudulent Credit Card at Grocery Store A**

32. Based on information from the River Forest Police Department, on or about April 1, 2017, a male individual attempted to purchase a \$50 gift card from Grocery Store A. The cashier at Grocery Store A noticed that the number embossed on the credit card did not match the number that the cash register read from the electromagnetic strip on the back of the card. According to the police report, as the cashier called for a manager's assistance, the male individual took the gift card out of the cashier's hand, hit the "approve" button on the register, and ran out of the store with the gift card.

33. I have reviewed images of the surveillance video from Grocery Store A. I am familiar with YORK's appearance from my review of prior arrest photographs from the Chicago Police Department as well as photographs from the Illinois Secretary of State that are associated with YORK's state identification card. Additionally, I have conducted surveillance of YORK on several occasions. Based on



my familiarity with YORK's appearance, the individual who purchased the \$50 gift card on April 1, 2017 was Cameron YORK.<sup>5</sup>

34. According to information that the River Forest Police Department received from Grocery Store A, the credit card used by YORK had a credit card account number of 454638xxxxxxx5431. Additionally, according to Grocery Store A, that same credit card account number was used in thirty-nine separate transactions at multiple locations of Grocery Store A's chain on April 1, 2017.

35. According to a law enforcement database, credit card account number 454638xxxxxxx5431 was issued by HSBC Bank PLC, based in the United Kingdom.<sup>6</sup>

36. Based on my training and experience, individuals who use fraudulent credit cards sometimes use those credit cards to purchase gift cards which can be used at a later date or sold to other individuals.

### **3. YORK's Use of a Suspected Fraudulent Credit Card During Law Enforcement Surveillance**

37. On April 7, 2017, law enforcement agents conducted surveillance of YORK at the 7000 block of West Grand Avenue, Chicago ("Prior Residence"), an apartment building in Chicago believed to be YORK's residence at the time of the

---

<sup>5</sup> According to the River Forest Police Department records, the manager and cashier at Grocery Store A were shown a six-photo array that included a photograph of YORK and were unable to identify YORK as the individual who purchased the gift card in the transaction described above.

<sup>6</sup> To date, law enforcement has not obtained records relating to this credit card from HSBC Bank PLC in the United Kingdom. According to the HSBC Bank PLC website, an individual is only eligible for an HSBC Bank PLC credit card if the individual is a "resident of the United Kingdom, Channel Islands, or Isle of Man." See <https://www.hsbc.co.uk/1/2/credit-cards>, last visited on July 2, 2017.

surveillance.<sup>7</sup> At approximately 11:00 a.m., YORK<sup>8</sup> exited the Prior Residence building and got into a car with an unknown female.

38. Law enforcement agents then followed YORK for several hours. During their surveillance of YORK, they observed YORK go into number of banking and retail establishments in the Illinois suburbs of Chicago, including: a TCF Bank in River Forest, a Jewel Osco in North Riverside, a Jewel Osco in Stickney, a Jewel Osco in Hickory Hills, a Jewel Osco in Palos Heights, a Walgreens in Alsip, and a Walgreens in Oak Lawn. The agents concluded their surveillance at approximately 3:20 p.m.

39. During this surveillance, an IRS-CI Special Agent followed YORK into the Jewel Osco in Stickney; with YORK was a second male, Individual C. The IRS-CI Special Agent observed Individual C attempt to purchase gift cards, cupcakes, and Lysol spray at one of the store's registers. The agent observed Individual C attempt to use multiple credit cards to purchase the items, but it appeared to the Special Agent that the credit cards were not authorized because he observed Individual C leave the register without purchasing the items. During the attempted sale, the agent saw YORK nearby in one of the aisles, talking on a cell phone.

---

<sup>7</sup> As explained below, YORK fraudulently used the personal identification of Victim E.C. to rent the Prior Residence in E.C.'s name and to establish a utility account at the Prior Residence in the name of E.C.

<sup>8</sup> Law enforcement agents who were familiar with YORK's appearance from prior arrest photographs observed the individual exiting the building and believed he was YORK based on his appearance.



40. Following the surveillance on April 7, 2017, I obtained transaction records and surveillance video from a representative of Walgreens regarding the transaction that took place in the Walgreens in Alsip. I am familiar with YORK's appearance from YORK's arrest photos, and viewed the surveillance video and observed an individual believed to be YORK making purchases at the Walgreens. At 2:27 p.m., YORK bought a phone charger for \$27.49, and paid for it using a credit card. YORK walked away from the register, and returned at approximately 2:30 p.m. YORK then bought a \$50 Visa gift card and paid for that gift card using the same credit card. YORK then attempted to purchase another \$50 Visa gift card using the same credit card, but that transaction was declined. According to a law enforcement database, the credit card that YORK used was issued by HSBC Bank PLC in the United Kingdom.<sup>9</sup>

41. Law enforcement agents are in the process of obtaining additional records from the other banks and retailers visited on April 7, 2017 to determine if additional fraudulent credit cards were used by YORK or Individual C, or if bank accounts were opened or utilized by YORK or Individual C.

---

<sup>9</sup> To date, law enforcement has not obtained records relating to this credit card from HSBC Bank PLC in the United Kingdom. As noted above, according to the HSBC Bank PLC website, an individual is only eligible for an HSBC Bank PLC credit card if the individual is a "resident of the United Kingdom, Channel Islands, or Isle of Man." See <https://www.hsbc.co.uk/1/2/credit-cards>, last visited on July 2, 2017.

**C. YORK's Use of Chicago Parking Meters and Square, Inc. to "Test" Credit Cards**

**1. YORK's Fraudulent Use of Chicago Parking Meters**

42. Based on my training and experience, individuals who possess stolen or fraudulent credit cards often "test" the credit cards by making small-dollar charges, such as parking meter charges, to see if the credit card company will authorize payment to the retailer. If the credit card company authorizes payment, the individual possessing the card will then know the credit card is an active credit card that can be used to make larger fraudulent charges. Individuals with stolen or fraudulent cards often want to "test" the cards to ensure that they do not use a credit card at a retailer that will be declined, which could draw attention to the user and may result in the retailer calling law enforcement.

43. On April 7, 2017, law enforcement agents conducted surveillance of YORK at an apartment building where YORK previously resided on the 7000 block of West Grand Avenue, Chicago ("Prior Residence"). I walked past the Prior Residence building on foot at approximately 8:53 a.m. and observed an individual standing outside the building, inserting a credit card into a Chicago parking meter machine. Based on my familiarity with YORK's appearance, I believe the individual I saw appeared to be YORK.

44. Based on records obtained from Chicago Parking Meters LLC, the operator of the parking meter, five different credit cards were "swiped" in the meter between 8:52 a.m. and 8:54 a.m. on April 7, the date and time period of the



surveillance. Each attempted transaction was in the amount of \$1.00. Three of the credit cards were declined by the issuer, and two were authenticated.<sup>10</sup>

45. On May 25, 2017, law enforcement agents conducted surveillance of YORK at the Prior Residence building. At approximately 9:24 a.m., a law enforcement officer observed an individual at a parking meter outside of the Prior Residence building, and based on his familiarity with YORK's appearance, believed that individual was YORK.

46. The law enforcement agent observed YORK insert more than one credit card into the parking meter. Based on my experience, Chicago parking meters provide a customer with a parking receipt that is to be placed on the dash of the car. While YORK was at the parking meter, I saw the Subject Vehicle parked on the street. YORK did not approach the Subject Vehicle and did not place anything on the dash. Approximately five minutes later, I saw YORK get into the Subject Vehicle and drive away.

47. As described above, based on my training and experience, individuals who possess stolen or fraudulent credit cards often "test" the credit cards by making small-dollar charges to see if the credit card company will authorize payment to the retailer.

---

<sup>10</sup> I checked a law enforcement database and these cards were issued by HSBC Bank PLC, in the United Kingdom. To date, no records have been received from HSBC Bank PLC regarding these accounts. As noted above, according to the HSBC Bank PLC website, an individual is only eligible for an HSBC Bank PLC credit card if the individual is a "resident of the United Kingdom, Channel Islands, or Isle of Man." See <https://www.hsbc.co.uk/1/2/credit-cards>, last visited on July 2, 2017.

48. Based on records obtained from Chicago Parking Meters LLC, the operator of the parking meter, six different credit cards were “swiped” in the meter between 9:22 a.m. and 9:24 a.m. on May 25, the date and time period of surveillance. Each attempted transaction was in the amount of \$1.00. All six credit card transactions were declined by the credit card issuer. According to a law enforcement database, all six credit cards were issued by Capital One NA.

**2. YORK’s Fraudulent Use of Square, Inc.**

49. The following paragraphs are based on information available from Square’s website ([www.squareup.com](http://www.squareup.com)), last visited by me on June 25, 2017:

a. Square is a financial services and mobile payment company that markets several software and hardware payments and products. Square provides “Point of Sale” software, which is a service that lets individuals and businesses process credit card payments, charging credit cards and causing the funds to be deposited into that individual or business’s bank account. In essence, Square allows users to use their cellular phones or tablets to facilitate credit card payments.

b. Square sells devices (a “Square Reader”) that plug into a phone or tablet, and which can read the information found on an electromagnetic strip found on a credit card. This device allows a user to “swipe” a credit card.

c. The Square Reader works on most mobile devices, including cellular telephones and tablets. According to the website, Square’s software does not work on non-mobile devices such as laptop computers.



d. In order to use the Square Point of Sale software, a user must setup an account with Square. The following information is required to create a Square account: full legal name, Social Security number, U.S.-based bank account, date of birth, and U.S. home mailing address. Square also requests users provide additional information, including the user's phone number.

50. According to records provided by Square in response to a subpoena, Square user ID 22557842 ("Square Account 1") was established on July 28, 2016 in the names of Cameron YORK and "Curtis Jones". The information provided to Square for YORK includes an address in the 4900 block of Race Avenue in Chicago, a date of birth of 03/xx/1991,<sup>11</sup> and a Social Security number ending xx3981. The identity information provided for "Curtis Jones" includes the same address in the 4900 block of Race Avenue in Chicago, and a date of birth of March 20, 1990. Square was also provided a telephone number for this account which ends in 9273 (Subject Phone 3). According to the information provided by Square, the Square account is linked to a TCF Bank account in the name of "Curtis Jones."<sup>12</sup>

51. According to Illinois Secretary of State records, YORK has a current Illinois identification card listing the same address in the 4900 block of Race Avenue

---

<sup>11</sup> YORK's date of birth is redacted for purposes of this affidavit.

<sup>12</sup> According to records from TCF Bank, the residential address associated with this account is the same address in Glendale Heights, Illinois, that was on the "Curtis Jones" identification card provided by YORK to the Chicago Police Department in February 2017, except that the TCF Bank account records show an apartment number for this address, while the identification card does not have an apartment number. According to a law enforcement database, the social security number provided to TCF Bank upon account opening is not assigned to YORK or to an individual named "Curtis Jones."

as was provided to Square, and also bearing a date of birth of 03/xx/1991, the same date of birth listed in the records for Square Account 1. The card was issued in March 2017 and expires in March 2023. According to law enforcement databases, YORK's Social Security number ends xx3981.

52. As noted in above, on February 10, 2017, YORK was arrested by the Chicago Police Department and was in possession of a State of Illinois identification card in the name "Curtis Jones", bearing a date of birth of March 20, 1990. This is the same date of birth that was provided to Square for the identity information of "Curtis Jones" for Square Account 1, the Square account in the names YORK and "Curtis Jones."

53. According to records provided by Square, from the time period between July 28, 2016 and January 23, 2017, Square Account 1 had approximately 9,174 attempted credit card transactions totaling approximately \$59,474. Of these transactions, approximately 87% were not authorized. According to Square records, the reasons for non-authorization included the notations "pickup card (lost or stolen card)" or "do not honor." Based on my training and experience, credit card issuers will stop authorization for payments for card that have been reported to the credit card company as being lost by the user or stolen from the user.

54. According to an employee of Square, Square froze Square Account 1 on August 3, 2016, meaning that the credit card transactions that are authorized for payments would not be released to the bank account linked to the Square account. However, according to the Square employee, the user of YORK's account could still



submit credit card charges through the Square software to see if the transaction would be authorized, and the credit would be charged by Square if authorized, but the freeze would prevent funds from being released to the bank account associated with the Square account. As of January 25, 2017, the account in the name of YORK and "Curtis Jones" was deactivated by Square.

55. According to records provided by Square, for Square Account 1 approximately 9,157 of the approximately 9,174 attempted credit card transactions were a transaction in which the credit card account number was obtained from a card's magnetic strip or chip reader, using a Square Reader or similar product. For the remaining transactions, the credit card numbers were manually entered by typing in the number.

56. According to records provided by Square, for each credit card transaction, Square records the longitude and latitude of the mobile device used for the credit card transaction. For YORK's account, the credit card transactions took place at a number of different places including: at what appear to be residential buildings in Chicago and the surrounding suburbs, in the parking lot of North Riverside Mall in North Riverside, Illinois, and at various points along Interstate I-290.

57. Based on my review of records from Square, it appears that approximately 78% of the attempted credit card transactions for Square Account 1 were in an amount ranging from \$1.00 to \$2.00.

58. For some of the credit card transactions where charges were authorized, the account holder later reported to the card issuer that the charge by Square Account 1 had been made without their authorization. For example, according to records provided by Affinity Plus Federal Credit Union, a debit card issued by the bank with a debit card account number ending in xx7096 was charged \$1.00 by Square Account 1 on or about August 12, 2016. According to Square records, this “swipe” took place in Chicago, Illinois. According to the bank records, on that same date, the account holder, Victim S.H., submitted to the bank a sworn affidavit stating that the \$1.00 Square charge was “unauthorized.”

59. Based on information provided by Square, on January 25, 2017, Square account number 25699869 (“Square Account 2”) was opened in the name of Victim E.C. and “Curtis Jones.” The information provided Square for Victim E.C. includes a social security number ending in 2483<sup>13</sup>, a listed address in the 7000 block of West Grand Avenue, Chicago (an address very similar to the Prior Residence<sup>14</sup>), and the phone number of Subject Phone 3 – the same phone number provided during the opening of Square Account 1. The information provided for “Curtis Jones” includes an address on the 4900 block of Race Avenue, Chicago, a date of birth of 03/xx/1991, and a social security number ending in 3981 – the birthdate, and social security number of YORK and the address on YORK’s Illinois Secretary of State identification

---

<sup>13</sup> As noted above, the social security number for the “Eric C.” with a Florida driver’s license ends in 2483.

<sup>14</sup> The address provided to Square was identical to the address of the Prior Residence, except the unit number for the Prior Residence is “3E,” while the unit number provided to Square was simply “3.”



card.<sup>15</sup> According to the user of their account, this account was a “catering” business and the business name was “Chef.” According to Square records, this account was frozen on January 26, 2017.

60. According to records received from Square for Square Account 2, there was one single credit card transaction for \$1.00 on January 26, 2017. According to the Square records, the issuer of the credit card declined the transaction. On that same date, the Square account was frozen. Based on the Square records, the single credit card transaction took place in Chicago, Illinois, at or near the location of the Prior Residence.

61. According to information provided by Victim E.C. on or about April 12, 2017, Victim E.C. told law enforcement he had never established or used a Square account.

62. According to records provided by Square, for Square Accounts 1 and 2, the credit card transactions were transmitted to Square from various Apple products, including iPhones and iPads. Square provided the unique UDID<sup>16</sup> for each of the eight separate Apple products used by Square Accounts 1 and 2. According to Square,

---

<sup>15</sup> According to records provided by Square, there was no bank account associated with Square Account 2.

<sup>16</sup> UDID is an acronym for “Unique Device Identifier,” which is a unique 40-digit letter and number combination assigned to any electronic device running an Apple operating system. According to the Apple law enforcement guide, an Apple device can be connected to a computer equipped with the iTunes software, and in the iTunes software the UDID number for the connected device will be displayed. See “Legal Process Guidelines, J. Other Device Information”, available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>, last visited on July 3, 2017. Based on my training and experience, a UDID number can be determined in this manner even if an iPhone is locked.

the eight unique UDID numbers are as follows: (1) CD9F66BB-D534-4523-BDC9-445566596201 (iPhone<sup>17</sup>); (2) 14AA895A-909B-42D9-8AF8-A044C158B5A0 (iPhone); (3) 25A27855-9EF9-4472-81AD-B33EE79860E9 (iPhone); (4) 9E6AA4D9-9100-4286-A9D5-7F0C2F60DA3D (iPhone); (5) 9947F969-659F-4720-B52A-CFB7C3971626 (iPhone); (6) 7F422D1E-0595-417B-B72F-A2B9E6952207 (iPad); (7) 072F8318-102E-49DA-8CE8-FE8701B1A661 (iPhone); (8) DE084E2A-0BB3-4D67-AC92-828CA4FB579E (iPhone). According to Square, the same iPhone bearing a UDID ending in 1626 was used to access Square Accounts 1 and 2. Additionally, the same iPad bearing a UDID ending in 2207 was used to access Square Account 1 and 2.<sup>18</sup>

63. On or about June 6, 2017, an employee of Square confirmed via e-mail that all of Square, Inc.'s servers are located in the state of California.

### **3. Examples of Fraudulent Use of a Credit Card Following a Square "Test"**

64. I am in the process of obtaining from credit card issuers records of credit card transactions for credit cards that were "tested" using York's Square account, as described above. I have reviewed the records received to date, and there are

---

<sup>17</sup> In addition to UDID, the Square records indicate whether the device is an iPhone or an iPad.

<sup>18</sup> Additionally, according to records received from Square another account with account number 26021946 (Square Account 3) was established in the name of YORK on February 10, 2017, listing the same birth date, address, and social security number for YORK as was provided in Square Account 1. For Square Account 3, a phone number was provided that was one digit different from Subject Phone 3. According to Square, this account was frozen on February 14, 2017, and there was only one attempted credit card transaction for Subject Account 3 during the four days the account was active. The transaction was for \$1.00, and the credit card issuer did not authorize the charge, with a stated reason of "Lost/Stolen-Card reported as Lost/Stolen." According to the Square records, Square Account 3 was accessed using an iPhone bearing UDID D1FA12C7-90B4-41D1-9A7B-71966D97731C.



numerous instances where a credit card statement shows that the credit card was charged a small amount, often \$1.00, by YORK's Square account. After that initial charge, there are additional charges at retailers, restaurants, and other businesses in the Chicago area.

65. For example, according to records received from Capital One, a Visa credit card with an account number ending in xx8455 was issued in the name of Victim V.S., with an address in New Jersey. Based on the account records, the credit card is a business credit card associated with a realtor.

66. According to records from Capital One, on or about August 23, 2016, in two separate transactions, Square Account 1 charged the credit card account with an account number ending in xx8455 in the amount of \$1.00 in each transaction. On that same date, the credit card was used approximately 52 times at Chicago-area drugstores, grocery stores, and other retailers, with a total amount charged of approximately \$11,529.49.

67. According to records from Capital One, the next day, on or about August 24, 2016, the credit card with an account number ending in xx8455 was again "tested" using Square Account 1 eight times, with eight charges using Square Account 1 in amounts ranging from \$1.00 to \$10.00. Additionally, the credit card was "tested" using a Chicago Parking Meter, where the credit card was used for a \$1.00 charge. On that same day, the credit card was used at a number of Chicago-area retailers, including: (1) two separate transactions at Bloomingdale's, totaling \$2,833.87; (2)

two separate transactions at Nordstrom, totaling \$ 1,422.23; and (3) one transaction at Solstice, a sunglasses retailer, totaling \$937.13.

68. Based on information provided by Bloomingdale's, the credit card with a card number ending in xx8455 was used to purchase, among other things, a pair of Giuseppe Zanotti brand shoes for \$1,095, and various Burberry brand items totaling \$1,278.

69. Based on information provided by Nordstrom, the credit card with a card number ending in xx8455 was used to purchase various items totaling \$1,422.23 in two separate transactions.

70. Based on information provided by Solstice, the credit card with an account number ending in xx8455 was used to purchase two pair of sunglasses totaling \$937.13. Solstice also provided me with copies of the surveillance video from the date and time that the credit card with an account number ending in xx8455 was used. I have reviewed the surveillance footage, and based on my familiarity with YORK's appearance, I believe the individual using the credit card with an account number ending in xx8455 was YORK.

71. Based on information provided by Square, for each of the Square credit card transactions for the account number ending in xx8455 on August 23 and 24, 2016, the "swipe" of that credit card took place using a mobile device located in Illinois.



72. To date, I have attempted to make contact with the realty business for which the credit card account was issued in the name of Victim V.S., but I have not yet interviewed anyone at the realty business about these credit card transactions.

73. As another example, according to records received from U.S. Bank, a Visa credit card with an account number ending in xx2002 was issued in the name of Victim K.A., with an address in Milwaukee, Wisconsin.

74. According to records from U.S. Bank, on or about January 12, 2017, Square Account 1 charged the credit card account with an account number ending in xx2002 in the amount of \$1.00. According to Square records, the "swipe" of the credit card occurred in Chicago. On or about that same date, the credit card was used at a Walgreens in Waukegan, Illinois, with a charge of \$105.95.

75. According to records provided by U.S. Bank, on or about February 9, 2017, Victim K.A. submitted a signed affidavit to the bank stating that she has "not participated in and have no knowledge of" the two transactions described in the above paragraph. Victim K.A. also checked a box stating "I am claiming that I have my Credit/Debit Cards in my possession and there are Unauthorized Transaction(s) on my account."

76. As a third example, according to records received from AlaTrust Credit Union, a Visa with an account number ending in xx5556 was issued in the name of Victim T.W., with an address in Talladega, Alabama.

77. According to records from AlaTrust Credit Union, on or about December 27, 2016, Square Account 1 charged the credit card account with an account number

ending in xx5556 twice, once in the amount of \$1.00 and once in the amount of \$5.00. According to Square records, both of the “swipes” of the credit card occurred in Chicago. On or about that same date, the credit card was used at a BP gas station in Westchester, Illinois with a charge of \$40.97.

78. According to records provided by AlaTrust Credit Union, on or about December 28, 2016, Victim T.W.. submitted a signed affidavit to the bank stating that “I certify I did not use and that I did not authorize anyone to use my card” for the three transactions described above. Victim T.W. further indicated her card had been in her possession the entire time.

**D. YORK’s Discussion of Credit Card Fraud and Display of Proceeds of Fraud on Social Media**

79. Based on information received from Instagram, an Instagram account with the handle “glo\_please\_” (Subject Account 1) was established on or about November 24, 2016. According to subscriber records, the name on the account is “Glo” and the registered email address is “curtisjones230@yahoo.com.”<sup>19</sup> As noted above, “Curtis Jones” is a known alias for Cameron YORK.

80. On June 26, 2017 and several dates prior, I have reviewed the publicly available posts on Subject Account 1. I observed several pictures that show only one individual in the frame; based on my familiarity with YORK’s appearance, that individual is YORK.

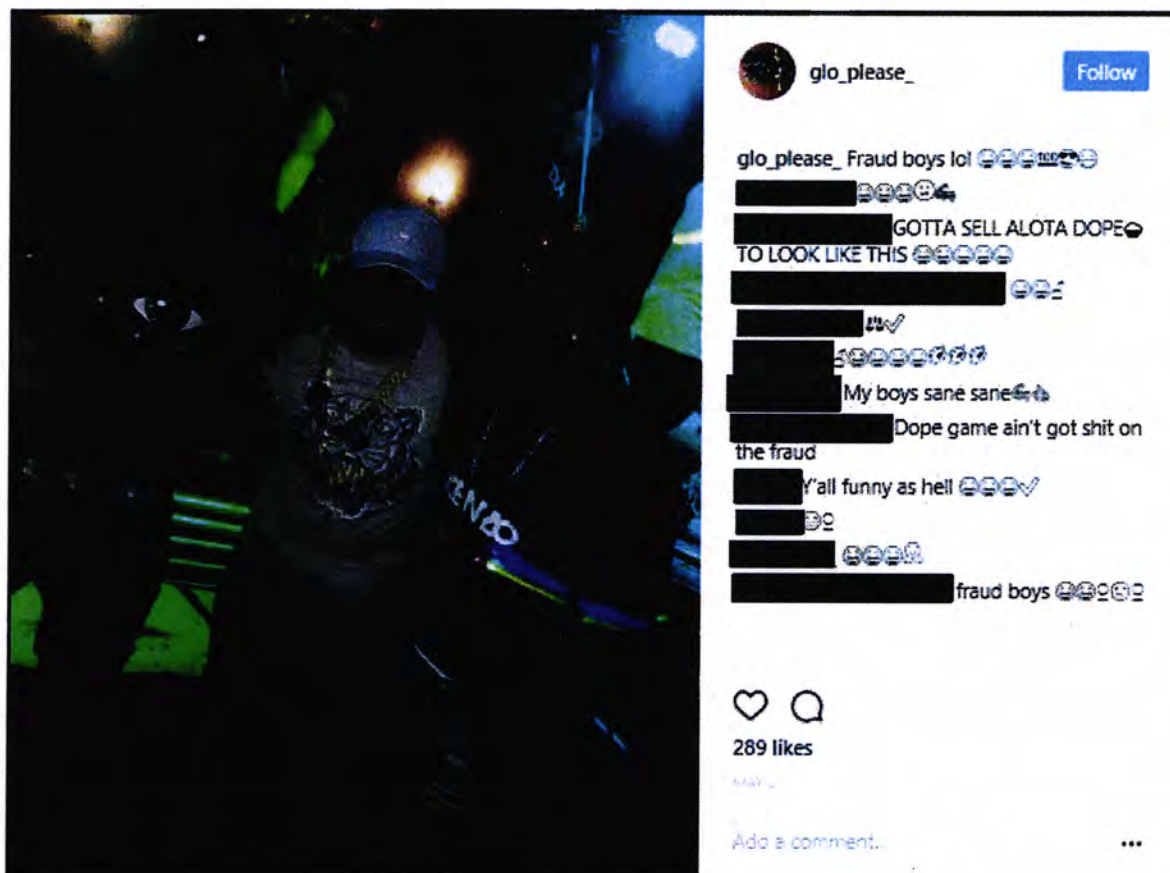
---

<sup>19</sup> The misspelling of “yahoo” as “yaho” is found in the documents from Instagram.



81. During my review of publicly-available posts on Subject Account 1, I observed posts which appear to explicitly reference credit card fraud. I observed the following posts:

a. Post dated May 2, 2017<sup>20</sup>:



As can be seen in the screenshot, the user of Subject Account 1 captioned this photograph "Fraud boys lol [laughing out loud]."<sup>21</sup> Another user commented "Dope

<sup>20</sup> Instagram usernames other than the username of Subject Account 1 have been redacted in this affidavit.

<sup>21</sup> Bracketed explanations of Instagram captions and comments in this affidavit are based on my training and experience.

game ain't got shit on the fraud.” Based on my familiarity with YORK’s appearance, the individual in the middle in this photograph appears to be YORK.

b. Post dated December 21, 2016:



Based on my familiarity with YORK’s appearance, the individual in this photograph is YORK. The caption reads “Fuck YO PLUG MINES BETTER LOL;” based on my training and experience, “plug” is a reference to an individual who provides fraudulent credit card information.

82. During my review of Subject Account 1, I observed several photographs of luxury goods and other items that are suspected to be proceeds of the credit card fraud. Based on my training and experience, individuals engaged in credit card fraud often use the fraudulent credit cards to purchase goods, including luxury goods, for



their own use and/or for sale to others. The following posts appear to show currency and goods that are suspected to be the proceeds of YORK's credit card fraud<sup>22</sup>:

a. Post dated January 21, 2017:



The shoes depicted in this photograph appear to be Maison Margiela brand. Based on information from the Maison Margiela website, visited on June 25, 2017, these retail price for these shoes is \$470.<sup>23</sup> Another Instagram user commented, saying "I need to fwu [fuck with you] when I get back to the states G, plug Shit."

b. Post dated April 8, 2017:

<sup>22</sup> Based on information from the Illinois Department of Employment Security, no employer reported that Cameron YORK earned wages in the third or fourth quarters of 2016 or the first quarter of 2017. The investigation, to date, has not uncovered any evidence that Cameron YORK is employed.

<sup>23</sup> See [https://www.maisonmargiela.com/us/maison-margiela/sneakers\\_cod11284837xp.html#dept=shsm](https://www.maisonmargiela.com/us/maison-margiela/sneakers_cod11284837xp.html#dept=shsm)



In the hands of this individual appears to be a stack of currency. The user of Subject Account 1 captioned this photograph "2 THINGS I DON'T STRESS ABOUT NO MONEY OR NO BITCH"

c. Post dated March 5, 2017:





This photograph shows bags and boxes from Louis Vuitton, a luxury brand selling shoes, clothes, luggage, accessories, and other items.

c. Post dated May 6, 2017:



The shoes in this photograph appear to be Balenciaga brand shoes; according to the Balenciaga website, accessed on or about June 25, 2017, the retail price for these shoes similar in appearance to these shoes is \$595.<sup>24</sup>

e. Post dated December 17, 2016:

<sup>24</sup>

*See*

[https://www.balenciaga.com/us/sneakers-shoes\\_cod11151782hx.html#/us/women/sneakers](https://www.balenciaga.com/us/sneakers-shoes_cod11151782hx.html#/us/women/sneakers)





The photograph in this picture appears to depict a black iPhone, along with a stack of U.S. currency. The caption reads "New iPhone 7 back down."

83. Additionally, as noted above, on April 1, 2017, YORK used a fraudulent credit card to purchase a gift card at Grocery Store A. On that same date, the user of Subject Account 1 posted the following photograph, which is publicly available:



Based on my familiarity with YORK's appearance, the individual in this picture is YORK. Additionally, based on my review of the surveillance images from Grocery Store A on this date, YORK is wearing what appears to be the same jacket, shirt, hat, and shoes in the surveillance images as he is in this photograph. The caption on this photograph reads, "I move Fast I JUST ACT SLOW." As noted above, on that date, while the cashier was attempting to call for a manager's assistance, YORK reached over, hit "approve" on the cash register, and ran out of the store with the gift card.

**E. Subject Phone 3 is Used by YORK**

84. As noted above, YORK provided a phone number ending in 9273 (Subject Phone 3) during the creation of Square Account 1, a Square Account in his own name. According to records provided by T-Mobile, Subject Phone 3 is a prepaid phone, and



T-Mobile does not maintain in their records the name of a subscriber associated with this account.

85. Based on records from T-Mobile, the IMEI of the phone associated with Subject Phone 3 changed to a new IMEI on February 12, 2017 – the same date that YORK was released from custody following his arrest for using the “Curtis Jones” identification, according to Chicago Police Department records. An “IMEI” is a unique number that can identify a particular mobile phone device. As noted above, law enforcement seized two cellular telephones during that arrest, and records showing a new IMEI on would be consistent with YORK obtaining a new cellular telephone to use with the account for Subject Phone 3.

86. On March 29, 2017, the government obtained authorization from Acting Chief Judge Rebecca R. Pallmeyer to obtain pen register and location information for a number of phones related to wire fraud, including Subject Phone 3, which is believed to be used by YORK. T-Mobile began providing real-time information on or about April 5, 2017. After the initial authorization, the government has obtained subsequent authorizations from Chief Judge Rubén Castillo to obtain pen register and location information, and T-Mobile has provided continuous location information for Subject Phone 3 since April 5, 2017.

87. The location information provided by T-Mobile is consistent with the law enforcement agents’ observations of the location of YORK during the surveillance of YORK on April 6, May 23, June 15 and June 21, 2017 that is described below. Additionally, the location information provided by T-Mobile is consistent with the law

enforcement agents' observations of the location of YORK during the surveillance of YORK on April 7 and May 25, 2017, as described above.

**F. YORK's Use of Victim's Personal Identification Information to Rent Apartments, Including the Subject Premises**

**1. Use of Victim E.C.'s Name to Rent Grand Ave. Apt.**

88. As described below, it is believed that YORK used the personal identification of Victim E.C. to rent an apartment located in the 7000 block of W. Grand Avenue in Chicago ("Prior Residence") which YORK has recently vacated before moving to the **Subject Premises**.

89. Based on records provided by ComEd on or about December 1, 2016, utilities were established at the Prior Residence in the name of Victim E.C., using the social security number of E.C.<sup>25</sup> According to the ComEd records, the phone number associated with the account is Subject Phone 3, a phone used by YORK.

90. Based on information provided by the property manager for the Prior Residence, on or about November 18, 2016, a lease was signed with the name of the tenant as Victim E.C., with a monthly rent for the Prior Residence of \$1775. The phone number provided by the tenant was Subject Phone 3.

91. Law enforcement conducted surveillance outside of the Prior Residence on several occasions in the spring and summer of 2017 and observed YORK leaving or entering the apartment building. For example, on April 6, 2017, a Chicago Police Department officer who is familiar with YORK's appearance from prior arrest

---

<sup>25</sup> I searched a law enforcement database to determine that the social security number associated with this account was assigned to Victim E.C.



photographs saw an individual he believed to be YORK exit the apartment building at approximately 12:40 p.m.

92. On April 12, 2017, two IRS-CI special agents interviewed Victim E.C., who lives in Florida. Victim E.C. confirmed that his social security number was the same number used to establish the ComEd account as described above. Victim E.C. stated he has never lived in Chicago and has not leased the Prior Residence nor did he set up ComEd utilities in his name at the Prior Residence. Victim E.C. explained that he suspected he was the victim of identity theft because he has received phone calls from car dealerships in the Chicago area asking about attempts to purchase a car in his name.

93. On or about April 4, 2017 Chicago Police Department received a police report from Individual D, a tenant in another unit in the Prior Residence building. According to that report, one of Individual D's neighbors had forcibly removed a security camera that Individual D had hung near the door of his unit.

94. I have reviewed the security footage provided by Individual D, which shows an individual reaching up and grabbing the security camera off of the wall. Based on my familiarity with YORK's appearance, the person who removed the security camera appeared to be YORK.

95. On or about June 21, 2017, I interviewed Individual D. Individual D identified the man in the security footage (YORK) as one of his neighbors, who lived in Unit 3E (the Prior Residence). Individual D further explained that on approximately June 13, 2017, he observed moving men taking items out of Unit 3E

and putting those items into moving trucks. Individual D indicated he believed that the man in the security footage (YORK) had moved out of his unit.

**2. YORK's Use of Personal Identification Information of Victim A.F. to Purchase a Vehicle and Rent the Subject Premises**

96. According to records from Dealership A, on or about May 15, 2017, Cameron YORK purchased from Dealership A in Wilmette, Illinois, a 2011 Jaguar XJL sedan, gold/silver color ("Subject Vehicle"). According to the records, YORK applied for an automobile loan using his true name, but falsely stated his social security number was a social security number that is actually assigned to Victim A.F.<sup>26</sup> According to Dealership A records, the loan application was routed to lenders using RouteOne software, and based on this loan application, Chase approved an automobile loan. Dealership A made a copy of YORK's state identification and retained that copy in their files.<sup>27</sup>

97. On June 7, 2017, I spoke with a representative of Route One, who confirmed that Route One's servers are located in Texas, meaning any transmission of a loan application from Illinois to a lender using Route One services would be transmitted via the server in Texas.

---

<sup>26</sup> I searched the social security number provided to the lender by YORK in a law enforcement database to determine that the number was assigned to Victim A.F.

<sup>27</sup> The copy of the Illinois state identification in the dealership's files lists an address in the 4900 block of Race Avenue, Chicago.



98. According to Illinois Secretary of State records, the Subject Vehicle is registered in the State of Illinois under the name of Cameron YORK.<sup>28</sup>

99. Additionally, based on records from ComEd, on or about May 31, 2017, a utility account was established in the name of CAMERON YORK for a residence at [REDACTED] (**Subject Premises**). According to ComEd records, the social security number provided during account opening is the social security number assigned to Victim A.F. Additionally, the birthdate provided during account opening is the birthdate of YORK.

100. I have attempted to make contact with Victim A.F, but to date, I have been unable to interview him regarding the automobile loan or the utilities account at the **Subject Premises**. According to a law enforcement database, Victim A.F. lives in Green Bay, Wisconsin.

**G. YORK Resides at the Subject Premises**

101. As noted, in May of 2017, YORK used the social security number of Victim A.F. to obtain an automobile loan. Based on records received from ComEd on June 30, 2017, on or about May 31, 2017, utilities were established in the name of "CAMERON YORK" at "[REDACTED]" (the

---

<sup>28</sup> According to Illinois Secretary of State records, the car is registered to an address in Glendale Heights, Illinois.

**Subject Premises**).<sup>29</sup> The ComEd records show that the social security number provided during the account opening is the social security number of Victim A.F.<sup>30</sup>

102. On July 1, 2017, I visited a website called "Hotpads" which is a publicly-available website listing apartments and other residences for rent. The "Hotpads" website listed the **Subject Premises** as available for rent; according to the website, the rental posting expired on May 22, 2017.<sup>31</sup> As noted above, Individual D, YORK's previous neighbor at the Prior Residence, observed moving vans moving items out of YORK's apartment on or about June 13, 2017.

103. Based upon my review of the listing on Hotpads, the rental listing contains several interior photos of Unit 2, the **Subject Premises**, which appears to be on the second floor of the duplex as there are photographs taken from the top of a staircase.<sup>32</sup>

---

<sup>29</sup> According to ComEd, the phone number provided during account opening is a phone number different than Subject Phone 3, which is believed to be used by YORK. However, as noted above, YORK has been arrested with more than one cell phone in his possession.

<sup>30</sup> According to a 2015 real estate listing for [REDACTED], the building has two units, one on the first floor and one on the second floor. See [https://www.redfin.com/IL/\[REDACTED\]/home/13335727](https://www.redfin.com/IL/[REDACTED]/home/13335727), last visited on July 2, 2017. Utility records indicate that Individual E has rented the first floor unit since at least March 1, 2017. According to records from ComEd on June 30, 2017, there are two utility accounts at the duplex: one account, activated on March 1, 2017, in the name of Individual E for unit "B" and the other account, for Unit 2, in the name of Victim A.F., which was activated on May 31, 2017. Additionally, according to records received from Comcast on June 16, 2017, there was no record of account for Unit 2, but there was an account for Unit 1, which was established in the name of an individual with the same last name as Individual E on or about March 9, 2017. According to the Comcast and ComEd records, the same phone number was provided by the account holders (who also share a last name) for the accounts for Unit B/Unit 1.

<sup>31</sup> See [https://hotpads.com/\[REDACTED\]-60165-sw1q9e/2/pad](https://hotpads.com/[REDACTED]-60165-sw1q9e/2/pad).

<sup>32</sup> Additionally, I viewed a listing on Hotpads for Unit 1 in the same building. See [https://hotpads.com/\[REDACTED\]-sw1q9e/1/pad](https://hotpads.com/[REDACTED]-sw1q9e/1/pad), last visited on July 2, 2017. According to the website, this listing expired on April 22, 2017. The photographs of



104. On June 15, 2017, at approximately 8:40 a.m., I drove by the **Subject Premises** and saw the Subject Vehicle parked outside. I then parked my car near the **Subject Premises**, though I could not see the front door of the **Subject Premises** from my vantage point. At approximately 11:07 a.m., I saw an individual I believed to be YORK walking towards the Subject Vehicle, coming from the direction of the **Subject Premises**. I observed YORK look into the window of the Subject Vehicle, and then walk back in the direction of the **Subject Premises**. At approximately 1:15 p.m., I observed an individual I believed to be YORK walk towards the Subject Vehicle from the direction of the **Subject Premises**. I saw YORK stand next to the Subject Vehicle and talk on the phone, and approximately two minutes later he got into the Subject Vehicle and moved the Subject Vehicle to the other side of the street, parking it on the same side of the street as the **Subject Premises**.

105. On June 21, 2017, at approximately 1:52 p.m., an FBI Special Agent who is familiar with YORK's appearance saw the Subject Vehicle pull up in front of the **Subject Premises** and park. An adult female was driving the vehicle, and exited the vehicle and went into the house. At approximately 1:54 p.m., the agent then observed an individual who he believed to be YORK exit the building containing the **Subject Premises**, walk over to the Subject Vehicle, and take what appeared to be

---

Unit 1 appear to be photographs of the first floor of the building. Additionally, while the listing for Unit 1 states that the unit includes off-street parking, the listing for Unit 2 states that the parking available for that unit is on-street parking. As noted below, surveillance has seen the Subject Vehicle parked on the street on more than on occasion.

grocery bags out of the trunk. The agent then observed YORK enter the building of the **Subject Premises**, carrying the grocery bags into the building. At approximately 2:10 p.m., the agent saw YORK exit the building of the **Subject Premises**, get into the Subject Vehicle, and drive away. At approximately 2:17 p.m., the agent observed the Subject Vehicle return to the 1500 block of 43<sup>rd</sup> Avenue and saw YORK exit the Subject Vehicle and enter the building of the **Subject Premises**.

106. On or about June 22, 2017, at approximately 1:36 a.m., a law enforcement officer familiar with YORK's appearance saw the Subject Vehicle drive up and park on the street in the 1600 block of N. 43<sup>rd</sup> Avenue, approximately eight houses away from the **Subject Premises**. At approximately 1:39 a.m., the law enforcement officer then saw an unknown female and an individual he believed to be YORK get out of the Subject Vehicle and enter the building of the **Subject Premises**.

107. I have reviewed location information provided by T-Mobile, and based on my review, the cell tower location information provided by T-Mobile is consistent with the presence of Subject Phone 3 at the **Subject Premises** during nighttime hours. For example, between June 21 and July 2, 2017 the location information provided by T-Mobile showed that Subject Phone 3 was in a location at or near the **Subject Premises** during at least part of the time period between 2:00 a.m. and 6:00 a.m., except for June 25, for which T-Mobile was unable to provide location information for Subject Phone 3 during the early morning hours.

108. Additionally, I have reviewed location information provided by T-Mobile, and the cell tower location provided by T-Mobile is consistent the moving date



of June 13, 2017 provided by YORK's former neighbor, Individual D. In early June, the location information provided by T-Mobile for Subject Phone 3 showed that the phone was frequently in an area consistent with the Prior Residence. According to the location information, Subject Phone 3 was in a location consistent with the Prior Residence at approximately 11:30 a.m. on June 13, 2017. Then, according to the location information, Subject Phone 3 was in a location consistent with the **Subject Premises** at approximately 5:00 p.m. on that same date, June 13, 2017. According to the location information, after 5:00 p.m. on June 13, 2017, Subject Phone 3 has frequently been in an area consistent with the **Subject Premises**, as described in the above paragraph. Since that date and time, Subject Phone 3 has not frequently been in a location consistent with the Prior Residence.

#### **H. Background on Fraudulent Credit Card Schemes**

109. Based on my training and experience, individuals who use fraudulent credit cards to obtain goods and gift cards often store those goods and gift cards at their residence.

110. Based on my training and experience, individuals engaged in credit card fraud and identity theft often maintain in their residences magnetic strip readers, magnetic strip re-encoders, embossing machines, and other tools used to alter credit cards. Additionally, such individuals often maintain the electronic devices used to alter credit cards and to make purchases with fraudulent credit cards and personal identification information of third-parties, including computers, tablets, and cellular telephones.

111. Additionally, based on my training and experience, individuals engaged in a financial fraud such as credit card fraud and identity theft often keep receipts and lists of credit card numbers, social security numbers, and other identification information in their residence.

**I. York's Use of Apple Products**

112. Based on the investigation, YORK has been known to use Apple products, including iPhones and iPads.

113. According to records provided by Square, credit card transactions were submitted to Square, using Square Accounts 1 and 2, by eight different Apple products, including iPhones and an iPad.

114. Additionally, as described above, during YORK's February 2017 arrest by the Chicago Police Department, YORK had on his person an iPhone.

115. As noted above, the user of Subject Account 1, believed to be YORK, posted a picture of what was captioned as a "New iPhone 7."

116. Based on records provided by T-Mobile, on or about May 23, 2017, YORK entered a T-Mobile store in North Riverside, Illinois and purchased an iPhone 7. The customer listed on the receipt<sup>33</sup> is "Cameron York." According to the receipt provided by T-Mobile, the phone number for this iPhone is (312) xxx-5531 (Subject Phone 4),<sup>34</sup>

---

<sup>33</sup> I have not yet obtained from T-Mobile the complete credit card account number that was used to purchase the iPhone.

<sup>34</sup> The full phone number is redacted for purposes of this affidavit. Based on my training and experience, during the execution of a search warrant, one way law enforcement agents identify whether or not a specific phone number is assigned to a mobile device is to call that phone number and see if the device will ring. Additionally, according to the Apple website, an Apple product can be connected to a computer which contains iTunes software, and in the



and the IMEI<sup>35</sup> for this iPhone is 355323087962939. I have reviewed surveillance video provided by T-Mobile and the individual who bought an iPhone in YORK's name appears to me to be Cameron YORK. In addition to the phone that he purchased, I also observed YORK take another phone in and out of his pocket and type on the screen while he was waiting to complete his transaction. I believe the second phone possessed by YORK was an iPhone because I could see what appeared to be the iPhone apple logo on the back.

**J. Probable Cause to Search Electronic Devices**

117. As noted above, based on my training and experience, individuals involved in credit card fraud offenses often keep lists of credit card numbers and personal identification, including keeping those lists on electronic storage media devices such as computers, laptops, cell phones, and tablets.

118. Further, based on my training and experience, individuals involved in identity theft and credit card fraud use the internet, including email, websites and chat-rooms, to obtain stolen identities and credit card numbers.

---

iTunes software the phone number for the connected device will be displayed. See <https://support.apple.com/en-us/HT204073>, last visited on July 3, 2017.

<sup>35</sup> Based on my training and experience, and IMEI is a uniquely-assigned number that can identify a specific device. According to the Apple website, an iPhone 7's IMEI number is printed on the SIM card tray on the side of the iPhone. See <https://support.apple.com/en-us/HT204073>, last visited on July 3, 2017. According to the Apple website, the SIM card tray can be easily opened using a paperclip. See <https://support.apple.com/en-us/HT201337>, last visited on July 3, 2017.

119. Additionally, as described above, the electronic strip on a credit card can be “re-encoded” using a credit card encoder and software found on a computer or other electronic device.

120. Based on my training and experience, individuals involved in criminal offenses commonly use e-mail and cellular telephones as a means to communicate. Individuals involved in criminal offenses also often store telephone numbers, e-mail addresses, and names or nicknames of fellow conspirators on their telephones, computers, and other electronic storage media devices. Additionally, text messages and e-mail messages stored in phones, computers, and other electronic storage media devices can provide information regarding the identities of, and the methods and means of operation and communication used by, the participants in the identity theft and wire fraud offenses. Specifically, in this case, YORK told a CPD officer that he saved in his phone the phone number of the source of the fraudulent identification and credit card. YORK also told the CPD officer that he corresponded with his source by text message and also by using an application in his phone.

121. Moreover, digital photographs located in the memory of smartphones, computers, tablets, and other electronic storage media devices may contain images of the tools or participants involved in the access device fraud and wire fraud offenses. Additionally, digital photographs stored in the electronic devices may contain images of the user, the user’s associates (including persons involved in or knowledgeable about the subject offenses), places frequented by the user of the phone leading up to and during the subject offenses, and locations and instrumentalities used in



committing the subject offenses. As discussed above, York appears in a number of photographs which reference credit card fraud and which were posted online. Further, based on my training and experience in credit card fraud cases, individuals who use fraudulent credit cards to purchase luxury goods and hotel rooms often take pictures of the luxury goods, and hotel rooms.

122. Additionally, information stored within an internet-capable electronic device may indicate the geographic location of the device and user at a particular time (e.g., location integrated into an image or video sent via email or text message to include both metadata and the physical location displayed in an image or video). Based on my training and experience, electronic devices often store information about wifi networks with which the phone receives or transmits data. Hotels and other business often have their own wifi networks, and smartphones, tablets, and computers may store information about those wifi networks which can provide a physical location of the user of that phone, tablet, or computer.

123. Based on my training and experience, individuals who purchase goods and services with fraudulent credit cards and/or personal identification information sometimes use the internet to complete such transactions. For example, individuals who make hotel reservations often make hotel reservations via the internet, and often receive e-mail confirmations of reservations and of hotel receipts at the conclusion of hotel stays. Such communications from hotels could be stored electronically on internet-capable electronic devices such as computers and smartphones.

124. As noted above, Square's credit card processing services can only be utilized by a mobile device, such as a smartphone or tablet. According to records from Square, eight separate Apple products were used to access Square Accounts 1 and 2.

125. Additionally, as noted above, Square Account 1 was associated with a TCF Bank account in the name of "Curtis Jones." Based on my training and experience, individuals who maintain bank accounts sometimes conduct bank transactions, such as electronic transfers of funds or electronic bill payment, on their personal computers using the internet.

## **II. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA**

126. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, tablets, and cellular telephones) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant.



This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

127. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

128. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

129. When searching the **Subject Premises**, it is likely that Apple brand devices, such as iPhones or iPads, will be found, as records from Square indicate that Square credit card processing services for the Square account were accessed using eight unique Apple products (iPhones and an iPad), and because YORK is known to carry an iPhone.<sup>36</sup>

130. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

131. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints, either their own or others’, that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to

---

<sup>36</sup> As described above, YORK is believed to possess and use iPhones, including as recently as May 23, 2017, when T-Mobile surveillance video shows YORK purchasing a new iPhone and using a second device that also appears to be an iPhone. An iPhone was seized from YORK during his February 2017 arrest, as described above. Additionally, as described above, YORK has used Apple products, including iPhones and an iPad, to access Square credit card processing services.



unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

132. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include when more than 48 hours have passed since the last time the device was unlocked. The Touch ID feature will also not work and entry of a passcode will be required if the device's user or someone acting on the user's behalf has remotely locked the device. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID, and execute the search authorized by the requested warrant, exists only for a short time (*i.e.*, 48 hours or less, or until the device is given a remote lock command). Touch ID also will not work to unlock the device if the device has been turned off or restarted (*e.g.*, if the device's battery becomes fully depleted), or after five unsuccessful attempts to unlock the device via Touch ID are made.

133. The passcode or password that would unlock any Apple devices found during the search of the Subject Premises is not known to law enforcement. Thus, it likely will be necessary to press the finger(s) of the user(s) of the Apple devices found during the search of the Subject Premises to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. In addition, I also know from my training and experience, as well as

from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offers users the ability to remotely erase the contents of such devices. Attempting to unlock the relevant Apple devices via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access or retrieve the data contained on those devices for the purpose of executing the search authorized by the requested warrant.

134. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock any Apple devices found in the **Subject Premises** as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

135. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of CAMERON YORK at the Subject Premises to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found at the **Subject Premises** for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by the requested warrant.



### III. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

136. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

137. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

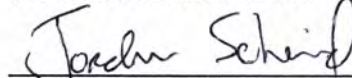
138. The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.



#### IV. CONCLUSION

139. Based upon the information set forth above, I submit that there is probable cause to believe that (a) Cameron YORK committed wire fraud, in violation of Title 18, United States Code, Section 1343; and (b) at the **Subject Premises**, there exists evidence, instrumentalities, contraband, and fruits of violations of Title 18, United States Code, Section 1343.

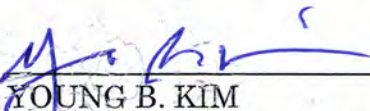
FURTHER AFFIANT SAYETH NOT.



JORDAN SCHEID

Special Agent, Internal Revenue Service –  
Criminal Investigation (IRS-CI)

SUBSCRIBED AND SWORN to before me on July 3, 2017.



YOUNG B. KIM

United States Magistrate Judge